REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicant has amended claims 23, and 27-28. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-31 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Examiner Objections - Claims

Claims 23 and 27 were objected to because of informalities. Again, the Applicant appreciates the Examiner's thorough review of the claims. The Applicant has amended the claims as suggested by the Examiner in order to correct the informalities. The Examiner's consideration of the amended claims is respectfully requested.

3.) Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Niemi et al. (RFC 3310,HTTP Digest Authentication Using AKA) in view of Reiche (6,092,196).

Applicants once again respectfully traverse the Examiner's rejection and submit the following arguments and clarification seeking the Examiner's favorable reconsideration.

Independent Claim 1 is reproduced below for the Examiner's review:

1. A method of generating a password for use by an end-user device (UE) to access a remote server, comprising:

a) sending a request for access from the UE to the remote server;
b) creating a temporary identity for the UE;
c) sending to an authentication node in the UE's home network details of the request for access;
d) at the authentication node or the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user passwords, including details of the temporary identity of the UE;

e) at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the identity of the UE ; and
f) storing the password and the temporary identity of the UE at the UE.

Applicants respectfully submit that, at least, steps d, e, and f as identified above are not anticipated or rendered obvious by the cited references.

The cited Reiche reference does indeed disclose a client, customer server, and a centralized authentication server. When the client attempts to gain access to the customer server, the customer serve in Reiche then reroutes the authentication request to the authentication server in order to authenticate the client. However, in Reiche, the actual "user id and password" must be communicated between the client and the authentication server. For example, Col. 5, lines 17-22 of Reiche clearly state that "the centralized authentication server then initiates the access grant control procedure in the form of an authentication challenge. In other words, the authentication server issues control data to the user's machine to invoke on the display screen a dialog box with user id and password fields that must be completed by the user (emphasis added)."

Accordingly, when the Reiche user attempts to gain access to a particular customer server, the customer server then involves a centralized authentication server which then issues control data to display the "log on box" onto the client's machine enabling the client to enter the user id and password for actual authentication.

However, the Reiche reference fails to anticipate or disclose the novel step (step D) of the "authentication node or the remote server" generating an end user password in accordance with the Hypertext Transfer Protocol (HTTP) Digest challenge using details of the temporary identity of the end-user device. In Reiche, it simply issues control data to the client's machine to display a regular "log on box" in which the client can then type in his or her user id and password. The Examiner cited Col. 5, lines 17-28 of Reiche therefore instead disclose a simple "user id & password log-on box" procedure and fails to anticipate or render obvious the recited step of "the authentication server or the remote server generating a Hypertext Transfer Protocol (HTTP) Digest challenge using

an algorithm capable of generating end-user passwords, including details of the temporary identity of the UE."

Additionally, Reiche likewise fails to disclose or teach the step (E) as recited above. The Examiner once again referred to Col. 5, lines 17-25 of Reiche as allegedly disclosing this step and Applicant fails to understand how the cited portion of Reiche could anticipate or render obvious the above limitations. It does not discuss generating any password other than asking the client to type in his or her user id and password. Therefore, it fails to disclose or teach how to generate a "password based on the HTTP Digest Challenge, said password being associated with the identity of the remote server and the identity of the UE" as claimed. No such password being associated with the identity of the remote server and the identity of the UE are ever generated by the Reiche invention.

Lastly, Reiche fails to disclose how the "generated password and the temporary identity of the UE are stored at the UE (recited Step F)." First of all, Reiche generates no new password in accordance with the teachings of the present invention. Accordingly, there is nothing for Reiche to store within the UE as claimed. Second, In Reiche, the Authentication Daemon in the customer server generates a unique 4 byte client ID to keep track of the authentication request to the centralized server. Even if the Examiner is correct in associating this 4 byte client ID as the "temporary UE identity" as claimed by the present invention, nothing in Reiche discloses or teaches that this unique ID is then stored at the UE. Instead, it is clear in Reiche that such information is stored "in a row of memory table 122" at the customer server.

Therefore, Applicants submit that at least steps D, E, and F of Claim 1 are not anticipated or rendered obvious by the cited references and is patentable over the cited references.

For similar reasons, Applicants submit that independent claims 15 and 18 are likewise not anticipated or rendered obvious by the cited references. All other remaining claims are dependent from now allowable independent claims and recite further limitations in combination with the novel elements thereof. Therefore, the allowance of all of the pending claims is respectfully requested.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

John C. Han
Registration No. 41,403

Date: April 17, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-7686
john.han@ericsson.com